Accelerating automotive cybersecurity

Your guide to winning trust at every turn

Contents

Accelerating automotive cybersecurity

The rise in connected and autonomous driving is unlocking significant new opportunities for manufacturers and consumers. To realize its potential, manufacturers need to be able to meet the increasing demands on cybersecurity in electrical and electronic (E/E) systems for automotive vehicles.

Rapid evolution

The automotive industry is experiencing rapid evolution. Ambitious innovation, cutting-edge technology, and growing consumer appetite for connected vehicles mean more opportunity and choice for suppliers, manufacturers, passengers, and users.

Connectivity and automation

This evolution is perfectly illustrated by increasing levels of vehicle automation, using artificial intelligence (AI) and machine learning (ML) to guide them safely in dynamic environments. Consumers also have greater levels of connectivity to their vehicle via mobile apps, giving them control of their vehicle's status and functions.

Expanding threat landscape

Running parallel to this progress is an ever-changing threat landscape. To stay ahead of these risks, organizations need cybersecurity strategies that are robust, rigorous, and consistent.

Rob Brown, Global Head of Automotive

"Building trust in the era of connected vehicles requires a lifecycle approach to automotive cybersecurity. Through this guide, and our partnership, we'll support you with standards-driven compliance to forge lasting trust with your customers, partners and stakeholders."

Your guide to achieving compliance and security

Connected vehicles provide safety, comfort and enriched travel experiences. However, they're vulnerable to cyberthreats throughout their lifecycle – from design to decommissioning. Personally Identifiable Information (PII), payment details, travel history, and location data can all be hacked and misused or manipulated. This can include denying users access to their vehicle or its systems.

Security as standard

That's why adopting a standards-driven approach to cybersecurity across the whole product lifecycle is crucial. It's the cornerstone of a secure and responsible connected automotive industry that's ready for the future.

We'll provide recommendations on how you can:

- actively mitigate digital risk across the automotive ecosystem;
- build trust throughout the vehicle lifecycle;
- strengthen supply chain confidence and collaboration;
- demonstrate your commitment to meeting global regulations.

By 2030, 95% of new vehicles sold globally will be connected, while the number in service will extend from 192 million in 2023 to 367 million by 2027.[1]

[1] Connected vehicles to surpass 367 million globally by 2027, Juniper, 2023

Increasing automation drives the need for stronger cybersecurity

Society of Automotive Engineers (SAE) Automation Levels

SAE Levels of Driving Automation™ from Level 0 (no driving automation) to Level 5 (full driving automation) illustrate the context for increased automotive cybersecurity.

SAE **J3016**™ LEVELS OF DRIVING AUTOMATION™

Learn more here: sae.org/standards/content/j3016_202104

	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
What does the human in the driver's seat have to do?	**You <u>are</u> driving** whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			**You <u>are not</u> driving** when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			**These are automated driving features**		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering **OR** brake/ acceleration support to the driver	These features provide steering **AND** brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example Features	• automatic emergency braking • blind spot warning • lane departure warning	• lane centering **OR** • adaptive cruise control	• lane centering **AND** • adaptive cruise control at the same time	• traffic jam chauffeur	• local driverless taxi • pedals/ steering wheel may or may not be installed	• same as level 4, but feature can drive everywhere in all conditions

[2] SAE levels of driving automation™ refined for clarity and international audience

Four key principles for automotive cybersecurity planning

Taking a holistic approach to planning automotive cybersecurity will help you build confidence and trust with your partners and customers. There are four key elements to consider, which you should think of as inter-connected: vehicle, lifecycle, supply chain, and regulations.

1 Connected vehicles

Anticipating sophisticated cyberthreats to the vehicle

OEMs and their suppliers should demonstrate robust measures against evolving cyberthreats across an increasing number of attack surfaces. Entry points such as apps, Bluetooth, Wi-Fi, telematics, and ports for on-board diagnostics mean that systems must be secured against best-practice standards.

2 Supply chain

Mitigating supply chain risk

Complex supply chains are vulnerable to disruption, from cybersecurity breaches to material shortages. The confidence to share sensitive data – from prototypes to software code – is built on trust. Standards and assurance help provide this trust.

3 Product lifecycle

Demonstrating whole-lifecycle cybersecurity protection

Cybersecurity systems need to cover the whole lifecycle of a vehicle and connected mobility assets, from design, build, and operation to maintenance (including over-the-air (OTA) updates) and end-of-life data cleansing. Rigorous planning, underpinned by standards, will provide complete end-to-end confidence.

4 Regulations and standards

Staying ahead of automotive regulations and standards

OEMs and suppliers are adapting to regulations and compliance deadlines, such as UNECE Regulation No. 155 (R-155) and No. 156 (R-156) in 2024. In parallel, standards bodies and industry groups are developing best practices to help suppliers achieve compliance and mitigate cybersecurity risks.

Five essential tools for building trust and compliance

As a globally recognized leader with deep cybersecurity expertise in the automotive industry, we help you embed comprehensive best-practice solutions for compliance and confidence. With training, audit, and accredited certification services, we support your efforts to meet global regulations, mitigate digital risk, and inspire trust.

On the next two pages, we share five essential standards and assessment schemes your organization should leverage to help you understand and embed best practice. These represent just a sample of the standards applicable to your sector.

68.5% of the C-Suite think there needs to be more understanding across the automotive supply chain of the implications of standards and what it will mean for their businesses.[3]

[3]Automotive threat intelligence on the road to cyber safety, Kaspersky, 2023

Five essential tools for building trust and compliance

1

Information Security Management Systems (ISO/IEC 27001)

A globally established and trusted standard for information security governance. It’s the foundational information security management systems standard, which opens doors to the responsible and secure use of AI, ML, and automation.

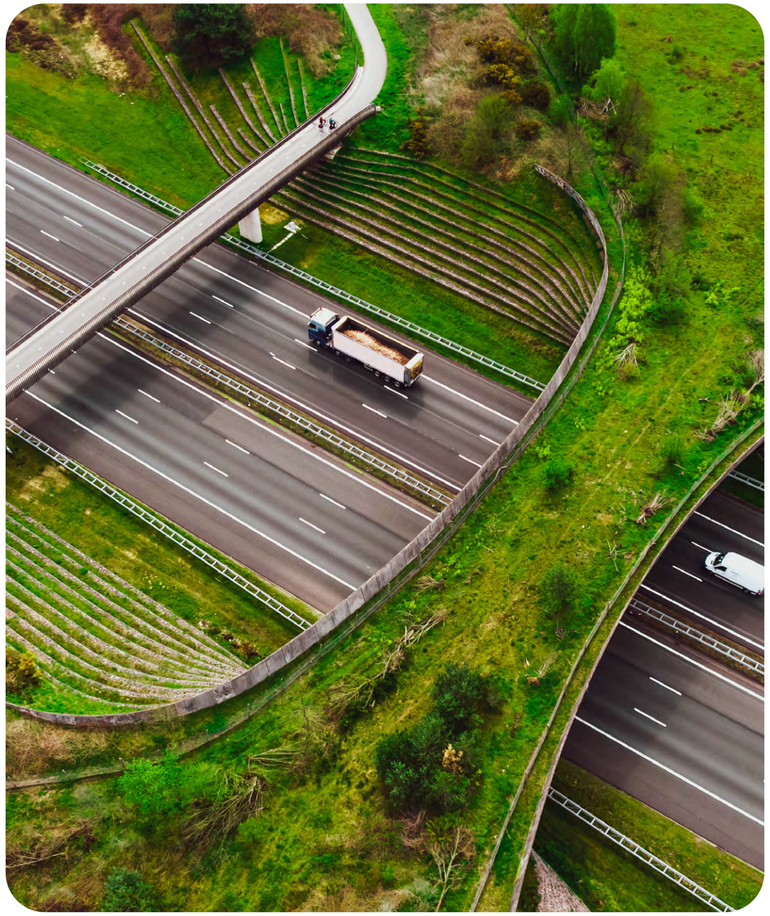
Find out more

2

TISAX Assessment

Developed by the automotive industry for the automotive industry, this information security assessment scheme is based on the requirements of ISO/IEC 27001. It unifies information security across three key domains and enhances trusted information exchange between supply chain partners, from OEMs through all tiers of suppliers.

Find out more



Five essential tools for building trust and compliance

3

Vehicle Cybersecurity Requirements (ISO/SAE 21434)

This standard specifies requirements for cybersecurity risk management throughout the whole lifecycle of electrical and electronic (E/E) systems in road vehicles, including all components and interfaces. Effective implementation of the standard helps you meet UNECE regulations R-155 (implementation of a cybersecurity management system) and R-156 (implementation of a software update management system).

Find out more

4

ENX Vehicle Cybersecurity (VCS) Audit Scheme

New in 2024, this scheme supports automotive suppliers who develop, produce, or maintain E/E systems for road vehicles. It provides standardized Cybersecurity Management System (CSMS) audits by implementing the guidelines for auditing cybersecurity engineering (ISO/PAS 5112) in the context of the ISO/SAE 21434 and UNECE R-155. A successful audit creates the foundation for trust and cooperation between supply chain partners.

Find out more

5

BSI Kitemark™ Certification for Secure Digital Applications

This BSI Kitemark™ certification proves that your organization has undergone rigorous and independent testing of its digital applications embedded in or remotely connected to a vehicle. It inspires trust by ensuring that robust controls meet industry standards including OWASP (The Open Web Application Security Project), ASVS (The Application Security Verification Standard) for web applications and MASVS (the Mobile Application Security Verification Standard).

Find out more

Building a robust cybersecurity ecosystem

Use our graphic on the following page to explore standards, frameworks, and solutions relevant to your role in the supply chain and product lifecycle. It incorporates the five best practices outlined in this guide, and additional related standards, to help you build a comprehensive toolkit for boosting digital trust.

> Automotive businesses know there is a problem but are currently struggling to decipher what to do about it.[4]

[4] Automotive threat intelligence on the road to cyber safety, Kaspersky, 2023

Automotive Cybersecurity Ecosystem

Product Lifecycle	**Design & Build**				**Operate & Maintain**			**Reuse & Recycle**	
Supply chain	**Tier 3** Part/HW/SW supplier	**Tier 2** Component supplier	**Tier 1** System supplier	**OEM** Auto maker	**Developer** Embedded SW, SaaS	**Processor** Data storage & processing	**Developer** Software update	**Processor** Factory reset/ data deletion	**Recycler** Recover and reuse
Products	Chips	PCBs	SatNav, ALKS, EMS	Vehicles User apps Dealer tools	Embedded software apps	Cloud storage	Patches, versions, security updates	Data in vehicle, apps, cloud	Chips, PCBs, systems, precious materials
Regulations	<<<		UN R155	>>>		UN 156	>>>	GDPR	>>>
OEM Flow Down	<<<			OEM flow down requirements for ISO/IEC 27001, TISAX and ENX VCS					>>>
Supplier goals	<<<			Compliance with regulations and customer requirements Eliminate unwanted checks from OEMs and customers Build a solid platform for technological advancement Mitigate against cyber risks (malware) and unauthorized access (hacking)					>>>
	<<<			**Standards, training, assessment, and certification supporting:** ISO/IEC 27001 – Information Security Management ISO/SAE 21434 – Vehicle Cybersecurity Management TISAX Assessment and ENX VCS Audit Scheme					>>>
BSI solutions	ISO/IEC 24089- Software Update for Vehicles BSI Kitemark™ for Secure Digital Applications				ISO/IEC 24089- Software Update for Vehicles BSI Kitemark™ for Secure Digital Applications	ISO/IEC 27017 - Infosec for Cloud Services ISO/IEC 27018 - PII in Public Clouds	ISO/IEC 24089- Software Update for Vehicles BSI Kitemark™ for Secure Digital Applications	ISO/IEC 27017 - Infosec for Cloud Services ISO/IEC 27018 - PII in Public Clouds	
Benefits	<<<			Build stakeholder trust: consumers, supply chain partners, and regulators					>>>

Progress towards a secure digital future

The approach we've shared in this guide can help you build a robust whole-lifecycle approach to cybersecurity that:

1. Actively predicts and mitigates digital risk.
2. Strengthens collaboration with supply chain partners.
3. Demonstrates compliance with regulations and OEM mandates.
4. Accelerates adoption of AI, ML, and automation technologies.

Keeping these principles in mind will help you stay ahead of evolving digital risk – essential to delivering positive impact and accelerating your business growth.

"The market for automotive cybersecurity is expected to reach **USD $9.7 billion by 2030.**[5]"

[5]'Cybersecurity in automotive: Mastering the challenge', McKinsey & Company

Your partner in progress

To find out more about our standards, training, audit, and certification services, visit our website.